(U) The Other Side of Open Source

FROM: ██████████████
SID OPSEC Program Manager (S02L3)
Run Date: 05/26/2005

Open Source is a resource for NSA... and for the enemy, too. (U//FOUO)

(U//FOUO) As you probably know by now, NSA is increasing the amount of open source available to intelligence analysts at an incredible rate. As Charlie Speight mentioned in his recent SID *today* column , the push for inclusion of this information is coming from the highest levels of our government. This is a wise choice, as the amount of information available via open source is overwhelming. However, have you ever stopped to think about what this means in terms of protecting **our** information?

(U//FOUO) Many of you have heard of a document called the " *Terrorist Training Manual* ", found in the home of a suspected al-Qaeda member in Manchester, England in May 2000. But did you know what that document has to say about open source information? Consider the following quote: "Using this public source openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy." In other words, without stealing a single document, tapping a single phone, or intercepting a single message, our adversaries can know exactly what we plan to do with a very high level of certainty.

(U//FOUO) So, what can we do? Despite this grim news, all is not lost. We can still conceal our vital secrets by protecting our critical information using the five steps of Operations Security (OPSEC). By identifying our critical information, analyzing the threat, analyzing our vulnerabilities, assessing our risk, and finally applying countermeasures, we can make it much more difficult for our adversaries to adversely affect our missions or our way of life. This is something we all have to work on as a team. We each have a responsibility to ensure that even our unclassified information does not get exposed to those without a need to know.